

IN THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

LISTING OF THE CLAIMS:

1. (Currently amended) A process for protecting a computer from hostile code, the process comprising [the steps of]:

defining at least two trust groups, each of the defined trust groups being characterized by a trust group value;

assigning objects and processes in the computer to one of said trust groups, irrespective of the rights of a user of said computer;

upon operation of a process over an object [or over a second process], comparing a trust group value of the process with a trust group value of the object [or with the trust group of the second process, and];

allowing the operation [according to the results of said comparing step] if the trust group value of the process is not smaller than the trust group value of the object; and

disallowing the operation if the trust group value of the process is smaller than the trust group value of the object.

2. (Currently amended) The process of claim 1 wherein a process is assigned upon creation to the trust group assigned to the passive code [starting] from which the process is created.

3. (Currently amended) The process of claim 1 further comprising [the step of] changing the trust group of [said] the process [after said operation] if the trust group value of the process is greater than the trust group of the object.

4. (Currently amended) The process of claim 1 further comprising [the step of] changing the trust group of said object or of said second process after said operation.

5. (Currently amended) The process of claim 1 further comprising, upon creation of an object by a process, [the step of] assigning said created object to the trust group of said process.

6. (Currently amended) The process of claim 1 further comprising, when said operation is allowed, [the step of] assigning said process to the trust group of said object or of said second process.

7. (Currently amended) The process of claim 1 wherein said trust groups are hierarchically ordered, and wherein [the step of] said allowing further comprises:

allowing said operation when the trust group of said process is higher or equal in said hierarchy than the trust group of said object or of said second process; and

denying said operation when the trust group of said process is lower in said hierarchy than the trust group of said object or of said second process.

8. (Currently amended) The process of claim 7 further comprising [the step of] assigning said process to the trust group of said object or of said second process after the operation is allowed.

9. (Original) The process of claim 1 further comprising:
defining at least two types of objects;
assigning objects to one of said types; and
wherein the step of allowing operation over an object is further carried out according to the type of said object.

10. (Previously presented) The process of claim 1 further comprising:
defining at least two types of processes;
assigning processes to one of said types, and
wherein the step of allowing operation of a process is further carried out according to the type of said process.

11. (Original) The process of claim 1, further comprising:
defining at least two types of operations; and
wherein the step of allowing operation of a process over an object or over a second process is further carried out according to the type of said operation.

12. (Original) The process of claim 1, further comprising:
defining at least two types of storage methods,
assigning a trust group to a type of storage methods; and
carrying out a storage operation for a process of a trust group according to the storage method assigned to the trust group of said process.

13. (Currently amended) A computer-readable medium comprising computer readable instructions for protecting a computer from hostile code, the instructions causing the computer to:
identify objects and processes within the computer;
define a table of at least two trust groups[, and]; and
assign objects and processes in the computer [being assigned] to one of said trust groups irrespective of the rights of a user of said computer; [and]
whereby upon operation of a process over an object, the computer is configured to:
compare a trust group value of the process with a trust group value of the object;
allow the operation if the trust group value of the process is not smaller than the trust group of the object; and

disallow the operation if the trust group value of the process is smaller than the trust group value of the object

[a controller configured to access said table and allow an operation of a process over an object or over a second process according to the results of a comparison of the trust group of said process and the trust group of said object or the trust group of said second process].

14. (Currently amended) The computer-readable medium of claim 13 further comprising instructions causing the computer to:

define a table of types of at least two types of objects, the objects in the computer being assigned one type; and

wherein the [controller] computer accesses said table for allowing said operation.

15. (Currently amended) The computer-readable medium of claim 13, wherein said table of trust groups is stored in a non-volatile memory.

16. (Currently amended) The computer-readable medium of claim [13] 14, wherein said table of types is stored in a non-volatile memory.

17. (Currently amended) The computer-readable medium of claim 13, further comprising instructions causing the computer to define a table of rules, and wherein said [controller] computer accesses said table of rules.

18. (Currently amended) The computer-readable medium of claim [13] 17, wherein said table of rules is stored in a non-volatile memory.

19. (Currently amended) The computer-readable medium of claim 13, wherein the computer is operatively coupled to a network, the network including a server, the table of trust groups stored in said server.

20. (Currently amended) A computer-readable medium according to claim [19] 14, wherein the computer is operatively coupled to a network, the network including a server, the [said] table of types is stored in said server.

21. (Currently amended) A computer-readable medium according to claim [19] 17, wherein the computer is operatively coupled to a network, the network including a server, the [said] table of rules is stored in said server.

22. (New) A computer-readable medium containing a computer readable instructions for protecting a computer from hostile code, the instructions causing the computer to:

define at least two trust groups, each of the defined trust groups being characterized by a trust group value;

assign objects and processes in the computer to one of said trust groups, irrespective of the rights of a user of said computer;

upon operation of a process over an object, compare a trust group value of the process with a trust group value of the object;

allow the operation if the trust group value of the process is not smaller than the trust group of the object; and

disallow the operation if the trust group value of the process is smaller than the trust group value of the object.